UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA

Case No. 12-20646 CR-MOORE / TORRES

18 U.S.C. § 371
18 U.S.C. § 1030(a)(2)(C)
18 U.S.C. § 1030(c)(2)(B)(i) and (iii)
18 U.S.C. § 1028A
18 U.S.C. § 2
18 U.S.C. § 982

UNITED STATES OF AMERICA

vs.

KENNETH WAHLER,
a/k/a "Ken Wahler,"

Defendant.
_____/

appear – SDFL. 9/21/12 @ 1:30 PM

INDICTMENT

The Grand Jury alleges that:

GENERAL ALLEGATIONS

At all times relevant to this Indictment:

1. Team Enterprises Incorporated ("TEI") was a marketing company which served the beverage/liquor industry by customizing marketing and advertising campaigns for various companies across the United States. TEI was incorporated in Massachusetts and was headquartered at 110 East Broward Boulevard, Suite 2450, Fort Lauderdale, Florida.

2. TEI's computers were protected computers in that they were used in or affecting interstate or foreign commerce or communication as defined in 18 U.S.C. §1030(e)(2)(B).

3. TEI maintained an email server at PEER 1, a company which provides Internet hosting services to clients all across the United States. PEER 1 provided TEI a managed hosting service for its email server. A managed hosting service is a type of Internet hosting in which the client leases an entire server which is not shared with any other clients. TEI's email server at PEER 1 was housed at a data center located at 2300 NW 89th Place, Miami, Florida. To gain access to the TEI's email server, TEI's employees were required to use individual usernames and passwords.

4. TEI established and maintained a file transfer protocol ("FTP") server at its headquarters, located at 110 East Broward Boulevard, Suite 2450, Fort Lauderdale, Florida. The FTP server allowed TEI employees to access training and internal process documentation from anywhere in the world. To gain access to the FTP server, TEI's employees had to connect through the Internet to a specific Internet protocol address then use a specific username and password. This specific username and password were sent to TEI's employees via email to their individual email accounts on TEI's email server hosted at PEER 1.

5. Defendant **KENNETH WAHLER** was a software programmer who resided in the State of Maryland. In or around May 2003, TEI hired **WAHLER** as an independent contractor to assist with fixing a TEI computer program called the "Retail Trac Software." The software was to be used by TEI in coordinating client events. After the program was fixed, **WAHLER** hosted the Retail Trac Software for TEI on an Internet platform in Maryland for a monthly fee. TEI's employees gained access to the Retail Trac Software by using individual usernames and passwords. **WAHLER**, as host of the Retail Trac Software, was able to view this information.

6. **KENNETH WAHLER's** services were terminated by TEI on or about February 28, 2008.

7. During the time that **KENNETH WAHLER** worked with TEI, he was authorized by TEI to access the Retail Trac Software. **WAHLER** was not authorized to access any other TEI computer or server including TEI's email server hosted by PEER 1 and its FTP server located at its headquarters in Broward County, Florida.

8. An Internet Protocol address ("IP address") is a unique numeric address used to identify computers on the Internet. An IP address is a series of four numbers, each in the range of 0-255, separated by periods (e.g., 121.56.97.178). Every computer (or group of computers using the same account to access the Internet) attached to the Internet must be assigned an IP address which acts much like a home or business street address, enabling Internet sites to properly route traffic sent to and from the computer. When a message is sent, the IP address allows one to trace the message back from the computer that received the message to the IP address of the computer that sent the message. There are two types of IP addresses: dynamic and static. A static IP address is one that is permanently assigned to a given computer on a network. With dynamic IP addressing, however, each time a computer establishes an Internet connection, that computer is assigned a different IP address.

9. IP address 65.119.123.62 is owned and maintained by Qwest Communications, an Internet service provider. Chesapeake Marketing, located at 901 East Fayette Street, Baltimore, Maryland, was the subscriber for IP address 65.119.123.62 during the time period March 14, 2008, through February 28, 2009. Chesapeake Marketing is one of several companies which is a part of Chess Communications. **KENNETH WAHLER** worked at Chess Communications from approximately 2003 through at least January 30, 2009.

COUNT 1
Conspiracy
(18 U.S.C. § 371)

1. Paragraphs 1 through 9 of the General Allegations section of this Indictment are realleged and incorporated by reference as though fully set forth herein.

2. From in or around March 2008, and continuing through on or about January 26, 2009, in Miami-Dade and Broward Counties, in the Southern District of Florida, and elsewhere, the defendant,

KENNETH WAHLER,
a/k/a "Ken Wahler,"

did knowingly and willfully, that is, with the intent to further the objects of the conspiracy, combine, conspire, confederate, and agree with persons known and unknown to the Grand Jury to commit certain offenses against the United States, namely:

(a) to intentionally access a computer without authorization and exceed authorized access, and thereby obtain information, the value of which exceeded $5,000, from a protected computer, and the offense was committed for the purpose of commercial advantage and private financial gain, in violation of Title 18, United States Code, Section 1030(a)(2)(C), (c)(2)(B)(i) and (iii); and

(b) to knowingly possess and use, without lawful authority, a means of identification of another person, during and in relation to a felony violation of Title 18, United States Code, Chapter 47, to wit, Title 18, United States Code, Section 1030(a)(2)(C), (c)(2)(B)(i) and (iii), in violation of Title 18, United States Code, Section 1028A(a)(1).

PURPOSE OF THE CONSPIRACY

3. The purpose of the conspiracy was for the defendant and his coconspirators, to unlawfully enrich themselves by: (a) stealing the usernames and passwords of TEI employees to gain access to TEI's email and FTP servers, and to obtain TEI's emails, email attachments, and other business documents containing TEI's confidential and proprietary information, including client proposals and presentations; and (b) stealing that information to obtain a private financial gain and commercial advantage for themselves.

MANNER AND MEANS OF THE CONSPIRACY

The manner and means by which **KENNETH WAHLER** and his coconspirators sought to accomplish the objects and purpose of the conspiracy included, among other things, the following:

4. **KENNETH WAHLER** obtained the usernames and passwords of TEI employees and made unauthorized access and exceeded authorized access to TEI's email server using these usernames and passwords.

5. **KENNETH WAHLER** downloaded without authorization the TEI employees' emails, email attachments, and other business documents, containing TEI's confidential and proprietary information.

6. **KENNETH WAHLER** forwarded the falsely and fraudulently obtained TEI employees' emails, email attachments and other business documents containing confidential and proprietary information to a coconspirator.

7. **KENNETH WAHLER** made unauthorized access and exceeded authorized access to TEI's FTP server and downloaded business documents containing TEI's confidential and proprietary information.

8. **KENNETH WAHLER** forwarded the business documents downloaded from TEI's FTP server to a coconspirator. **WAHLER** did so to obtain a commercial advantage and private financial gain for himself and his coconspirator.

OVERT ACTS

In furtherance of the conspiracy and to effect the objects and purpose thereof, the following overt acts, among others, were committed and caused to be committed in Miami-Dade and Broward Counties and elsewhere, by at least one coconspirator:

1. On or about April 3, 2008, **KENNETH WAHLER**, using the username and password of TEI employee J.V., accessed TEI's email server and forwarded an email with the subject heading "TEAM lead status call" dated April 3, 2008, along with its attachments to his email address "Kwahler@salestrac.com." The email and attachments contained confidential, proprietary information of TEI.

2. On or about April 3, 2008, **KENNETH WAHLER** forwarded an email with the subject heading "TEAM lead status call" dated April 3, 2008, along with its attachments to a coconspirator.

3. On or about January 6, 2009, **KENNETH WAHLER** gained access to TEI's FTP server and downloaded five files containing TEI's confidential and proprietary information relating to a presentation which was to be made to a client.

4. On or about January 21, 2009, **KENNETH WAHLER**, using the username and password of TEI employee D.R., accessed TEI's email server and downloaded an attachment dated January 21, 2009, which contained confidential and proprietary information of TEI relating to an upcoming presentation to be made to a client.

5. On or about January 21, 2009, **KENNETH WAHLER** , sent an attachment dated January 21, 2009, which he had downloaded from TEI's email server, to a coconspirator.

All in violation of Title 18, United States Code, Section 371.

COUNTS 2-3
Fraud in Connection with Computers
(18 U.S.C. § 1030(a)(2)(C), (c)(2)(B)(i) and (iii))

1. Paragraphs 1 through 9 of the General Allegations section of this Indictment are re-alleged and incorporated by reference as though fully set forth herein.

2. On or about the dates listed below, in Miami-Dade County, in the Southern District of Florida and elsewhere, the defendant,

KENNETH WAHLER,
a/k/a "Ken Wahler,"

intentionally accessed a computer, that is, TEI's email server, without authorization and exceeded authorized access, and thereby obtained information, the value of which exceeded $5,000, from a protected computer, as more particularly described below, and the offense was committed for the purpose of commercial advantage and private financial gain:

Count	Approx. Date	IP Address Used	TEI Information Obtained
2	April 3, 2008	65.119.123.62	Email with attachments of TEI employee J.V.
3	January 21, 2009	65.119.123.62	Email attachment of TEI employee D.R.

In violation of Title 18, United States Code, Sections 1030(a)(2)(C), 1030 (c)(2)(B)(i) and (iii), and 2.

COUNT 4
Fraud in Connection with Computers
(18 U.S.C. § 1030(a)(2)(C), (c)(2)(B)(i) and (iii))

1. Paragraphs 1 through 9 of the General Allegations section of this Indictment are re-alleged and incorporated by reference as though fully set forth herein.

2. On or about January 6, 2009, in Broward County, in the Southern District of Florida, and elsewhere, the defendant,

KENNETH WAHLER,
a/k/a "Ken Wahler,"

intentionally accessed a computer, that is, TEI's FTP server, without authorization and exceeded authorized access, and thereby obtained information, the value of which exceeded $5,000, from a protected computer, and the offense was committed for the purpose of commercial advantage and private financial gain, in violation of Title 18, United States Code, Sections 1030(a)(2)(C), 1030 (c)(2)(B)(i) and (iii), and 2.

COUNTS 5-6
Aggravated Identity Theft
(18 U.S.C. § 1028A(a)(1) and (c)(4))

1. Paragraphs 1 through 9 of the General Allegations section of this Indictment are re-alleged and incorporated by reference as though fully set forth herein.

2. On or about the dates set forth below, in Miami-Dade County, in the Southern District of Florida, and elsewhere, the defendant,

KENNETH WAHLER,
a/k/a "Ken Wahler,"

during and in relation to a felony violation of Title 18, United States Code, Chapter 47, that is, Fraud in Connection with a Computer, Title 18, United States Code, Section 1030(a)(2)(C), as set forth in

Counts 2 and 3 of this Indictment, did knowingly transfer, possess and use, without lawful authority, a means of identification of another person, to wit, the username and password of TEI employees, as set forth in the individual counts below:

COUNT	APPROX. DATE	MEANS OF IDENTIFICATION
5	April 3, 2008	J.V.'s username and password
6	January 21, 2009	D.R.'s username and password

In violation of Title 18, United States Code, Sections 1028A(a)(1), (c)(4) and 2.

FORFEITURE
(18 U.S.C. 982)

1. The allegations of this Indictment are re-alleged and by this reference fully incorporated herein for the purpose of alleging forfeiture to the United States of America of certain property in which the defendant **KENNETH WAHLER** has an interest.

2. Upon conviction of a violation of Title 18, United States Code, Sections 371 or 1030, the defendant shall forfeit all of his respective right, title and interest to the United States in any property constituting, or derived from, proceeds the defendant obtained directly or indirectly, as the result of such violation.

All pursuant to Title 18, United States Code, Section 982(a)(2)(B), as well as the procedures set forth at Title 21,United States Code, Section 853.

A TRUE BILL

/s/ Kenneth Nichols

WIFREDO A. FERRER
UNITED STATES ATTORNEY

Lois Foster-Steers

LOIS FOSTER-STEERS
ASSISTANT UNITED STATES ATTORNEY